

IN THE CLAIMS:

Please amend the claims as follows:

1. (currently amended) A method for managing cryptographic keys that are specific to a personal device [[(100)]], comprising: the method being performed at a secure processing point(150) arranged in communication with the personal device, characterised in that the secure processing point performs the steps of:

retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from a read-only storage [[(120)]] of an integrated circuit chip [[(110)]] included in the personal device [[(100)]];

the secure processing point storing a data package in the personal device, the data package including at least one cryptographic key;

receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device [[(100)]], which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage [[(125)]] of the chip [[(100)]];

associating the unique chip identifier with the received backup data package; and

storing the backup data package and the associated unique chip identifier in a permanent public database [[(170)]].

2. (currently amended) The method as claimed in claim 1, wherein the secure processing point further performs the further steps of:

associating a unique device identity with the unique chip identifier;

signing the result of said associating step-with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;

storing the certificate in the device; and

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.

3. (original) The method as claimed in claim 1, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

4. (original) The method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

5. (original) The method as claimed in claim 4, wherein the symmetric key is generated as a function of a master key and the unique device identity.

6. (original) The method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair.

7. (original) The method as claimed in claim 6, wherein the private/public key pair either is:

generated by the secure processing point during assembly of the device; or

generated and stored in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package.

8. (original) The method as claimed in claim 2, wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network.

9. (currently amended) A system for managing cryptographic keys that are specific to a personal device, ~~the system including comprising:~~
at least one personal device, ~~[(100)]~~ and
a secure processing point ~~[(150)]~~, which secure processing point is arranged in communication with the personal device, ~~characterised in that:~~
wherein the at least one personal device includes an integrated circuit chip ~~[(110)]~~ with a unique chip identifier in a read-only storage ~~[(120)]~~ and a unique secret chip key in a tamper-resistant secret storage ~~[(125)]~~;
wherein the secure processing point includes processing means(155)a processor configured for retrieving the unique chip identifier and for storing a data package in the device, the data package including at least one cryptographic key;
wherein the at least one personal device includes processing means(127)a processor configured for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point; and
wherein the processing meansprocessor of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database ~~[(170)]~~.

10. (currently amended) The system as claimed in claim 9, wherein the ~~processing means (155)~~processor of the secure processing point [(150)] further is arranged for:

associating a unique device identity with the unique chip identifier;

signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;

storing the certificate in the device; and

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.

11. (original) The system as claimed in claim 9, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

12. (original) The system as claimed in claim 11, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

13. (original) The system as claimed in claim 12, wherein the symmetric key is generated as a function of a master key and the unique device identity.

14. (original) The system as claimed in claim 11, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair.

15. (currently amended) The system as claimed in claim 14, wherein the ~~the processing means-processor~~ of the secure processing point either is:

arranged for generating the private/public key pair during assembly of the device;
or
arranged for retrieving the private/public key pair from a secure database
[[(140)]], in which the key pair has been stored in advance before assembly of the device, in which latter case the secure processing point further is arranged for removing the key pair from the secret database after reception of the backup data package.

16. (original) The system as claimed in claim 9, wherein the personal device is a wireless communications terminal and the unique device identity an identifier which identifies the wireless communications terminal in a wireless communications network.

17. (currently amended) A method of recovering a backup data package of a personal device [[(100)]], which backup data package has been assembled and stored in accordance with claim 1, the method including the steps of comprising:

reading a unique chip identifier from a read-only storage [[(120)]] of the personal device [[(100)]];
transmitting the chip identifier to a public database [[(170)]];
receiving from the public database the backup data package corresponding to the transmitted chip identifier; and
storing the received backup data package in the personal device.

18. (currently amended) A personal device [[(100)]] ~~managing cryptographic keys that are specific to the personal device, characterised in that the personal device includes~~comprising:

an integrated circuit chip [[(110)]] with a unique chip identifier in a read-only storage [[(120)]] and a unique secret chip key in a tamper-resistant secret storage [[(125)]];

~~processing means (127)~~ a processor configured for outputting the unique chip identifier; and

a memory means (130) for storing a received data package including at least one cryptographic key; and

~~processing means (127)~~ wherein the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database [[(170)]].

19. (currently amended) The personal device as claimed in claim 18, wherein the personal device includes a read-only memory [[(120)]] storing a manufacturer public signature key, andwherein the memory means (130) for storing the received data package is further for storing a received certificate, which corresponds to a certificate stored in association with the backup data package in the public database and which has been signed with a manufacturer private signature key corresponding to the manufacturer public signature key.

20. (original) The personal device as claimed in claim 18, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

21. (original) The personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

22. (original) The personal device as claimed in claim 21, wherein the symmetric key is generated as a function of a master key and the unique device identity.

23. (original) The personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair.

24. (original) The personal device as claimed in claim 18, wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network.

25. (currently amended) A secure processing point [[(150)]] for managing cryptographic keys that are specific to personal devices, ~~the secure processing point being capable of communicating with a personal device (100), characterised in that the secure processing point includes processing means (155) for comprising:~~

a processor configured for:

retrieving a unique chip identifier from a read-only storage [[(120)]] of an integrated circuit chip [[(110)]] included ~~by the~~in a personal device [[(100)]];

storing a data package including at least one cryptographic key in the personal device;

receiving an encrypted version of the data package, in the form of a backup data package, from the personal device in response to the stored data package; and

storing the received backup data package in association with the unique chip identifier in a permanent public database [[(170)]].

26. (currently amended) The secure processing point as claimed in claim 25, wherein the ~~processing means~~ (155)processor is further ~~is~~-arranged for:

- associating a unique device identity with the unique chip identifier;
- signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;
- storing the certificate in the device; and
- storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.